

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

21



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/748,654 | 12/22/2000 | Daryl Carvis Cromer | RPS919990119US1 | 4774 |

7590 07/15/2004

Andrew J. Dillon
FELSMAN, BRADLEY, VADEN, GUNTER & DILLON, LLP
Suite 350 Lakewood on the Park
7600B North Capital of Texas Highway
Austin, TX 78731

EXAMINER

HQ, THOMAS M

ART UNIT PAPER NUMBER

2134

DATE MAILED: 07/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

X

| | | | |
|------------------------------|--------------------------------------|--------------------------------------|--|
| Office Action Summary | Application No. 09/748,654 | Applicant(s) CROMER ET AL. | |
| | Examiner Thomas M Ho | Art Unit 2134 | |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
 - If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
 - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
 - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 22 December 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-16 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-16 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-16 are pending.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-16 are rejected under 35 U.S.C. 102(e) as being anticipated by Arnold, US patent 6,175,924.

In reference to claim 1:

Arnold discloses a method in a computer system for generating a certificate for use only within said computer system to authenticate operations internal to said computer system, said method comprising the steps of:

- Establishing a security subsystem within said computer system, where the security subsystem is the mechanism used to authenticate application programs with the computer system.

Art Unit: 2134

- Establishing a master key pair including a master private key and a master public key, where a private key pair and public key pair are established. (Column 5, lines 30-42)
- Storing said master private key in a protected storage within said security subsystem, wherein said master private key is inaccessible outside of said security subsystem, where the master private key is stored in secure persistent storage. (Column 5, lines 30-35)
- Supplying a target public key, where the public key is supplied when the keys are established.
- Requesting generation of a self-verifying certificate, where generation of a self verifying certificate occurs when a program asks the operating system to allocate a new persistent data area.
- Prompting a user for an authentication code in response to a request for generation of said certificate, where the prompt for the authentication code is automatic, and the operating system looks up the name of the program and the owner name field, labels used in the authentication process. (Column 6, lines 23-29)
- Generating a self-verifying certificate utilizing said target public key and said master key pair only in response to a correct entry of said authentication code, said certificate used only internally within said computer system, where the certificate is recovered or “generated” from the validation of the signature, (Column 5, line 65 – Column 6, line 5) and where Arnold discloses a method

Art Unit: 2134

where the certificate is used only internally within a computer system (Column 2, lines 50-55)

In reference to claim 2:

Arnold (Column 6, lines 23-29) discloses the method according to claim 1, further comprising the step of storing said authentication code in said security subsystem, where the authentication code is stored in a persistent data area with a permanent unalterable owner name field, where this persistent data area is part of the program authentication secure subsystem.

In reference to claim 3:

Arnold (Column 6, lines 23-29) discloses the method according to claim 2, further comprising the step of prohibiting an alteration of said authentication code after said authentication code is stored in said security subsystem, where the authentication code is stored in a persistent data area with a permanent unalterable owner name field, where this persistent data area is part of the program authentication secure subsystem.

In reference to claim 4:

Arnold (Column 6, lines 30-41) discloses the method according to claim 2, further comprising the step of prohibiting access to said authentication code to devices outside of the said security subsystem after said authentication code is stored in said security subsystem, where programs outside of access realm are prohibited from accessing any data which doesn't belong to it, including the authentication code.

Art Unit: 2134

In reference to claim 5:

Arnold (Column 5, lines 65 – Column 6, line 11) discloses the method according to claim 1, further comprising the step of determining a certificate identifier after a correct entry of said authentication code, said certificate identifier uniquely identifying said certificate.

In reference to claim 6:

Arnold (Column 5, lines 60 – Column 6, line 11) discloses the method according to claim 1, further comprising the steps of:

- Said security subsystem generating security data for said certificate after a correct entry of said authentication code, where the subsystem generates security data by decrypting the signature and recovering the hash, after the authentication code (the owner name field, and the program name is retrieved) and name matching needs to be done.
- Said security subsystem hashing said security data, where the security data is hashed. (Column 6, lines 5-11)
- Said security subsystem encrypting said security data utilizing said master private key to create a signature, where the security subsystem originally used the private key to create the signature. (Column 5, lines 32-43)
- Said security subsystem appending said signature to said security data to create said certificate, where the subsystem originally appended the signature to the program name and the program object. (Column 5, lines 38-53)

Art Unit: 2134

In reference to claim 7:

Arnold(Column 5, lines 16-21) discloses the method according to claim 1, further comprising the step of storing said certificate along with a certificate identifier in said computer system, where the certificate identifier is the name which must be unique within the domain of names that will be certified by that authority so that it may be used as an identifier.

In reference to claim 8:

Arnold(Column 5, line 43 - Column 6, line 18) discloses the method according to claim 1, further comprising the steps of

- receiving information within an appended certificate, where the information received in the authentication process is an appended certificate with the program object and name appended. (Column 5, lines 56-65)
- requesting authentication of a signature included within said appended certificate, where it is the signature that undergoes the authentication process. (Column 5, lines 65 – Column 6, line 18)
- said security subsystem reading said master public key from said protected storage, where the public key is stored in places where it is expected the private key will be used (Column 5, lines 35-38), and since the private key is used within the security subsystem, the public key will be located there as well.
- said security subsystem using said master public key to decrypt said signature, where the public key is used to decrypt the signature.

Art Unit: 2134

- said security subsystem determining whether said signature is authentic (Column 6, lines 5-18)

Claim 9-16 is rejected for the same reasons as claim 1-8, respectively.

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- US patent 5,844,986 discloses a BIOS that is updated with the use of a digital certificate, and is another example of a certificate designed solely for the internal use of a computer system.
- US patent 6,233,685 discloses a method of certificate based authentication and verification between devices. (not computer systems)
- US patent 6,519,700 discloses a method of creating a self protecting document through the use of signatures and certificates.
- US patent 6,615,350 discloses certificate authentication between libraries and modules that are being executed.

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas M Ho whose telephone number is (703)305-8029. The examiner can normally be reached on M-F from 8:30am – 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached at (703)308-4789. The fax phone numbers


Art Unit: 2134

for the organization where this application or proceeding is assigned are (703)746-7239 for regular communications and (703)746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)306-5484.

TMH

July 9th 2003


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100